SOLUTION BRIEF

FortiGate NGFW による キャンパスネットワークの保護

フォーティネットの次世代ファイアウォールである FortiGate NGFW で、組織は IT アーキテクチャにセキュリティを組み込むセキュリティ ドリブン ネットワークを構築できるようになります。

概要

建物が増えても同じネットワークを使用するためには、建物間を接続したり保護したりする必要があります。新たなキャンパス展開モデルは、こうした企業や教育機関の敷地内に建物が増築された際に役立ちます。キャンパスネットワークセキュリティの役割は、インターネットをはじめ、データセンターや複数のクラウドに展開されたアプリケーションへの安全なアクセスを提供することであり、非常に重要だと言えます。適切に行えば、内外の脅威（暗号化されたフローに潜むランサムウェアやコマンド & コントロール攻撃など）からネットワークを効果的に保護することができます。境界コントロールを迂回しようとする明らかな侵入を検知、最小化、阻止することで、キャンパスへの攻撃的侵入を防ぐことができるため、役割としては非常に重要になりますが、これだけではありません。

ネットワーキングとセキュリティのコンバージェンスの高速化

昨今のネットワークは非常に動的です。最新のネットワークで特に困難な特性の 1 つは、リモートでの仕事やキャンパス内での移動における、従業員のモビリティ度です。企業は、さまざまなエッジをキャンパスを超えて拡張しているため、いろいろな意味で中心となるのは境界ではなくユーザーであり、ユーザーの利用環境に影響を与えることなく保護する必要があります。また、デバイスの急増や場所に縛られない働き方のモデルにより、こうしたユーザーが増えるほど攻撃対象領域が劇的に増大します。現在のキャンパスネットワークセキュリティでは、トランザクション中に場所を移動してもアプリケーション、ワークフロー、および他のアクティビティをエンドツーエンドでシームレスに追跡し、ユーザーがどこにいても対応できることが求められています。

こうした特定の場所に対する従来のセキュリティモデルからのパラダイムシフトにおいては、キャンパスネットワーク、オフプレミス、オフネットワークに関係なく、ユーザーが移動する場所を問わず、より高い可視性とコンテキスト認識が求められます。認識度が高いほど、より多くの保護が可能になります。広範な可視性により、ネットワーク全体で強力なセキュリティ態勢の維持が可能になります。しかし、今日の高度で動的なネットワーク環境でプロアクティブな保護を実現するには、ネットワーキングとセキュリティを単一のデバイスに統合する必要があります。複雑なネットワークを保護しながら、生産性やユーザー環境を維持するためには、セキュリティ ドリブン ネットワーキングがますます不可欠になります。そこで、フォーティネットの FortiGate 次世代ファイアウォール（NGFW）が生み出す利点が非常に重要になるのです。

フォーティネットの FortiGate NGFW で、組織は IT アーキテクチャにセキュリティを組み込むセキュリティ ドリブン ネットワークを構築できるようになります。これにより、エッジの動的な変化に関係なく、あらゆる規模のエッジを保護できるようになります。さらに、可視性が向上し、一貫性のある組織的なエンドツーエンドポリシーが適用され、シームレスなユーザーエクスペリエンスを維持できるようになります。

フォーティネットの FortiGate NGFW は、世界で唯一のセキュリティプロセシングユニット（SPU）を搭載し、レイヤー 4 およびレイヤー 7 の高度なセキュリティ機能において、競合のファイアウォールの中でも業界トップの Security Compute Rating（セキュリティ計算処理評価）を実現しています。高度で完全に統合されたセキュリティ機能の強力なポートフォリオに加えて、フォーティネットの FortiGate NGFW には、統合型のゼロトラストネットワークアクセス（ZTNA）やリアルタイムビデオフィルタリングなど、最先端の FortiOS 技術による幅広いポートフォリオも搭載されています。さらに、人工知能 / 機械学習（AI / ML）を活用した FortiGuard サービスによりデバイスが強化され、直感的で自動化された管理しやすい NGFW プラットフォームが実現します。あらゆるデバイスに高度なイノベーションが搭載されているため、リスク管理、コスト削減、運用の合理化を向上させつつ、顧客はビジネスを拡大したり、中断を回避したりできるようになります。

フォーティネットの FortiGate NGFW ソリューションによる保護、統合、自動化

保護：ユーザーエクスペリエンスを損ねることなくキャンパスのセキュリティリスクを管理

キャンパスネットワークの保護は、IT チームにとって最優先事項です。しかし、可用性や適応性も同様に重要となります。また、攻撃を防御するという要件は変わりませんが、保護が必要な環境は変化しています。セキュリティおよびネットワークの管理者は、既知および未知の脅威を防御するために、あらゆるデバイスやユーザーなど、キャンパスにおける展開を完全に可視化する必要があります。これには、セキュリティとネットワークを 1 つのソリューションに統合し、ネットワーク上にあるものをすべて認識して対処できるようにする必要があります。デバイス、ユーザー、アプリケーションなどを、可視化すればするほど新たなコンテキスト情報を取得できるようになり、ポリシーを一層強力かつ効果的にすることが可能になります。しかし、可視化するだけでは必ずしも十分ではありません。FortiGate ファイアウォールはコンテキスト認識も可能なため、キャンパスネットワーク全体で強化されたセキュリティ態勢が実現し、維持されるようになります。

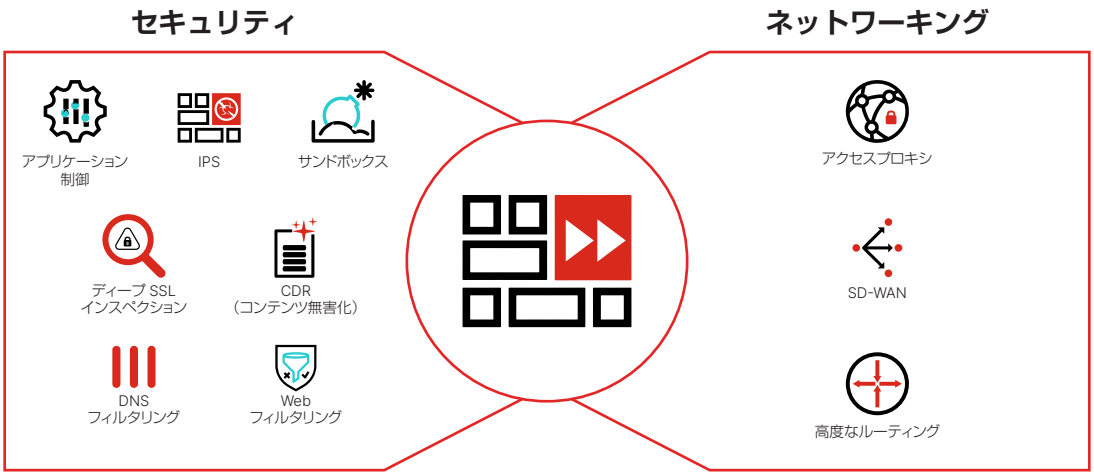
キャンパスネットワークに接続するデバイスが増えるほど、FortiGate ファイアウォールは、IoT デバイス、OT（オペレーショナルテクノロジー）環境、およびシステムやさまざまなユーザーを検出したり制御したりできるようになります。これは、デバイスの状況、オペレーティングシステム、パッチステータスなどを活用する確実なアクセス戦略によって実現されます。これにより、独自の ZTNA テクノロジーによる継続的なユーザー認証の実施が可能になり、キャンパス内外を移動する際に一貫したセキュリティポリシーをユーザーに提供できるようになります。

フォーティネットの FortiGate NGFW が提供する独自の戦略として、他にはキャンパスネットワーク全体での高度なインスペクション、動的なネットワークセグメンテーション、一貫性のあるポリシー適用により、攻撃対象領域を最小限に抑える機能があります。アクセスポリシーを実行したり、ユーザー毎やポートレベルで特定のリソースへのアクセスを制限したりできますが、これはフォーティネットのネットワークアクセス制御（NAC）ソリューションとの統合や、フォーティネットのスイッチやアクセスポイントにおけるセキュリティファブリックのネイティブ統合を利用して、詳細なアクセス制御を実現しています。また、相互接続されたセキュリティ製品から有益なテレメトリを収集したり対応したりすることにより、FortiGuard Labs が提供する実用的な脅威インテリジェンスを活用して、ゼロデイ脅威やランサムウェアをリアルタイムで検知および防止できるようになります。

統合：セキュリティ態勢を損ねることなく TCO を削減

業界で最も高速で価格競争力の高いソリューションがあれば、企業レベルのセキュリティでキャンパスネットワークの保護を向上させることができます。フォーティネットの FortiGate NGFW は、ネットワークの速度でプロセッサ集約型の機能を実行することができるため、組織は侵入防止システム（IPS）、SSL インスペクション、アプリケーション保護、Web フィルタリング、マルウェア防御などのサービスを FortiGate ファイアウォールに確実に統合できます。これらのサービスはすべて、スループットやネットワークの稼働時間を損なうことなく、同時に実行できます。これは、FortiGate の高度なセキュリティプロセッサが提供するパフォーマンス向上のイノベーションにより、すべて実現することが可能です。

こうした機能のあらゆる中心となるのが FortiOS です。このオペレーティングシステムは、セキュリティ ドリブン ネットワーキングのビジョンをサポートする製品のポートフォリオを、あらゆる環境やフォームファクターでそのまま利用できます。これにより、キャンパス、クラウド、広域ネットワーク（WAN）、さらには DevOps コンテナにも一貫したセキュリティを展開できるようになります。ネットワーク全体に単一のセキュリティシステムを導入することで、組織は単一のベンダーを通じて、ネットワークの実行、セキュリティ、サポートを優れたレベルで確立および維持できるようになります。



フォーティネットの FortiGate NGFW での機能統合

自動化：自動化による運用の簡素化により、可視性と制御性が向上

IT 部門の責任者たちは、拡大し続けるネットワークに適応し、拡張させていく必要に迫られています。これを安全に行うには、新たな保護対策を導入し、包括的なセキュリティを提供する必要があります。フォーティネットファブリックマネジメントセンター（FMC）が FortiGate ファイアウォールの展開をすべて制御することで、キャンパスネットワーク全体とすべてのネットワークエッジで、ファイアウォールとポリシー管理を合理化し、単一のコンソールからすべてのネットワーク保護デバイスに対して自動更新を提供することができます。

また、API やファブリックコネクタを FortiGate ファイアウォールと併用してセキュリティ態勢を簡素化することで、複数のクラウド間でセキュリティが標準化され、ユーザーがどこからでもアプリケーションにアクセスできるようになり、フォーティネット セキュリティ ファブリックのエコシステムによる運用の簡素化が実現します。

リアルタイム脅威インテリジェンス搭載の高度なファイアウォール機能

NGFW は、組織を内外の脅威から保護するために、ネットワークトラフィックをフィルタリングしてインスペクションを行う必要があります。今日の NGFW は、ゼロデイ攻撃、高度なマルウェア、ランサムウェアなどの脅威を特定してブロックする詳細なコンテンツインスペクション機能を備えています。また、SSL インスペクション（TLS 1.3 など）、アプリケーション制御、侵入防止、攻撃対象領域全体の完全な可視化も求められています。しかし、コロケーションやマルチクラウドの採用によって脅威の状況が急速に拡大し、増大する顧客やユーザーのニーズを満たすために企業が成長するにつれて、従来の NGFW ソリューションが大規模な保護に対応できなくなり、遅れを取っています。これにより、ユーザーエクスペリエンス、可視性、セキュリティ態勢の低下を招いてしまいます。今日の NGFW は、マルウェアをブロックするだけでなく、ネットワークに応じて拡張することも必要です。また、新たな脅威に対応する新しいネットワーク戦略が採用されたときに、脅威の状況に合わせて進化したり、ネットワークの安全性を維持したりするための柔軟性を持つことも必要になります。

フォーティネットの NGFW は、業界唯一の専用セキュリティプロセッサと堅牢な FortiOS のオペレーティングシステムに加えて、フォーティネットの高度な脅威インテリジェンスを提供するリサーチ部門である FortiGuard Labs との連携により、進化し続ける脅威環境の一歩先を行く上で最適な製品だと言えます。経験豊富な脅威ハンター、研究者、アナリスト、エンジニア、データサイエンティストなど、脅威の発見や分析を目的に設計された世界最先端の AI システムを活用する彼らの使命は、レポート、脅威の更新、主要な脅威研究者や法執行機関との連携、世界中に展開されている FortiGate デバイスへの毎日の脅威フィードなどを通して、今日の悪意のあるサイバー攻撃を防御するための業界最高レベルの脅威インテリジェンスを顧客に提供することです。こうした取り組みにより、フォーティネットのセキュリティ製品は脅威の識別や防御に関する最高レベルの情報を常に有し、フォーティネットの顧客に最新の脅威、キャンペーン、攻撃者、傾向を常に周知できるため、プロアクティブな対策で、環境のセキュリティを強化することができます。

すべてのユーザー、デバイス、エッジに高度なセキュリティを提供

フォーティネットの FortiGate NGFW は、包括的なエンタープライズクラスの可視性とセキュリティを提供し、あらゆる場所でユーザー、デバイス、エッジを保護します。フォーティネットの NGFW は、ゼロトラストアーキテクチャの展開でも有効であり、これによりユーザーは、継続的な認証、効果的かつ動的なコンプライアンス、適応可能なセキュリティ制御を通じて、いつでもどこからでも、業務に必要なアプリケーションやリソースに安全にアクセスできるようになります。

フォーティネットの業界をリードするセキュリティ ドリブン ネットワーキングのソリューションでは、セキュリティ、ネットワーキング、必須となる AI / ML 搭載の FortiGuard サービスを単一のプラットフォームにシームレスに統合します。この統合型のアプローチにより、現在のリスクをより適切に管理し、動的なネットワーク環境に適応するとともに、ビジネスの中断を回避し、複数のポイント製品の複雑さを排除して、業界で最も低い総所有コスト（TCO）を達成できるようにします。独自のセキュリティ ドリブン ネットワーキング戦略は、組織のネットワークインフラストラクチャとセキュリティアーキテクチャを緊密に統合することで、セキュリティ運用が損なわれたり、攻撃対象になるセキュリティの欠陥が生じたりすることなく、ネットワークの拡張や変更ができるようになります。

この新しい次世代のアプローチは、現在の極めて動的な環境を効果的に防御するために不可欠です。柔軟性の極めて高い境界全体で一貫性を持って適用させるだけでなく、ネットワーク自体にセキュリティを緊密に組み込んで防御することが重要です。

ビジネス運営のニーズに応えられるセキュリティ

現在の脅威環境は絶えず変化しています。分散型サービス拒否（DDoS）攻撃からランサムウェア、サイバー攻撃の頻度、規模、巧妙さまで、そのスピードが収まる気配はありません。すべての組織で、独自のネットワーク環境をサポートできるセキュリティが必要です。

1分間のダウンタイムやサービスパフォーマンスの低下など、ネットワークインフラストラクチャでたとえわずかでも中断が発生した場合、組織の評判、収益、さらには長期的な実行可能性が損なわれる可能性があるからです。多くの場合、壊滅的なサイバー攻撃は、ネットワークセキュリティツールが不十分だと見逃してしまい、最初のうちは軽微な侵入のように見えます。しかし、これが組織に壊滅的な罰金の支払や組織の完全な停止をもたらす可能性があります。問題は、従来の NGFW ソリューションがほとんど機能していないことです。

フォーティネットの FortiGate NGFW は、適応性の高いエンタープライズクラスのセキュリティを提供できる完全設計で、キャンパス、データセンター、リモートワーカー、マルチクラウド展開でのあらゆるユーザー、エッジ、規模に対して保護を提供します。従業員のハイブリッドワーキングやユーザーの期待の高まりにより、企業がデータセンターを超えて拡大するにつれ、キャンパスにおける展開もコアユーザーと同様に重要になります。セキュリティは、ユーザーが実行するさまざまなアプリケーション、ネットワーク、関連機能にシームレスなエクスペリエンスを提供する必要があります。

詳細については、Web サイト https://www.fortinet.com/jp/products/next-generation-firewall をご覧ください。

フォーティネットジャパン合同会社

〒106-0032
東京都港区六本木 7-7-7　Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ

SB-Protect-campus-deployments-Fortinet-FortiGate-202204-R1